Revisionsverkets ställningstaganden

Organisering av cyberskyddet

Revisionens mål var att utreda om cyberskyddet i statsförvaltningen har organiserats på ett maximalt effektivt och ekonomiskt ändamålsenligt sätt. Föremål för revisionen var statliga myndigheter som styr cyberskyddet (statsrådets kansli, finansministeriet, kommunikationsministeriet) och som sköter centraliserade cyberskyddsuppgifter och IKT-tjänster (Kommunikationsverkets Cybersäkerhetscenter, Statens center för informations- och kommunikationsteknik, Befolkningsregistercentralen). Hur styrningen fungerar bedömdes genom en granskning av statliga enheter som tillhandahåller e-tjänster (Befolkningsregistercentralen, Trafiksäkerhetsverket Trafi, Riksfogdeämbetet och justitieministeriet med ansvar för dess resultatstyrning samt Rättsregistercentralen, som är förvaltningsområdets IKT-servicecenter).

Operativt ledningsansvar vid omfattande cyberangrepp har inte fastställts

Arbets- och ansvarsfördelningen för att svara på cyberangrepp följer reglementet för statsrådet. I svårtolkade situationer har oklarheter kring hanteringen av cyberangrepp kunnat redas ut i förhandlingar mellan ministerierna. Under ett pågående cyberangrepp kan en förhandling dock ta mer tid än vad man har för att hålla situationen under kontroll. Planering och fördelning av operativt ledningsansvar för hantering av omfattande cyberangrepp kan bidra till snabbare reaktionstid samt ändamålsenlig resurstilldelning och koordinering av motåtgärder.

I dagens modell ansvarar varje ämbetsverk och inrättning för sitt cyberskydd. Det råder dock brist på yrkeskompetens inom detta område, vilket hämmar uppbyggnaden av ett cyberskydd med egna resurser eller genom inköp av tjänster. Verksamheter som statens ämbetsverk och inrättningar ansvarat för och skött själva har centraliserats till statens servicecenter genom servicecenterprojekt. Centraliseringen har medfört ett ökat behov av mer enhetlig och omfattande riskhantering. Praxisen för riskhantering varierar bland ämbetsverken. Oenhetlighet i riskhanteringen kan lämna hål i bl.a. skyddet av känsliga uppgifter. Det finns inte någon sammanställd information om e-tjänsterna i statsförvaltningen som pekar på att skydd och återställning av tjänsterna prioriteras när man svarar på ett omfattande cyberangrepp.

Ouppfyllda mål i strategin för cybersäkerhet

Programmet för genomförande av Finlands nationella strategi för cybersäkerhet (2013) har förstärkt cyberskyddet. Tack vare strategin uppmärksammades en enhetlig vision, integration av beredskapen i verksamheten och cyberskyddsförmågan.

Vissa mål i det första genomförandeprogrammet uppfylldes inte eftersom engagemanget för åtgärderna varierade och detta kunde inte heller påverkas centralt. I det nya genomförandeprogrammet ingår bara åtgärder som behöriga myndigheter och övriga aktörer visat ett engagemang för. Det finns ett beroendeförhållande mellan engagemang och resurstillgång. Man har försökt förbättra programuppföljningen för att ge statsledningen en bättre utblick över cybersäkerhetsläget.

Numera utgör samarbetet mellan Cybersäkerhetscentret och Försörjningsberedskapscentralen en viktig samlande kraft för utveckling av cybersäkerheten.

Oklart om finansieringslösningarna för cyberskyddet är ändamålsenliga

Skillnaderna i utvecklingen av cyberskyddet förklaras delvis av hur mycket utvecklingsresurser organisationerna har. Det finns dock vissa grundförutsättningar för cyberskyddet oberoende av statens och organisationens storlek. När tillgången till kritisk information och kompetens med tanke på cyberskyddet försvåras eller är otillräcklig hämmas skyddet mot cyberangrepp, som kan ha allvarliga och omfattande konsekvenser. Vikten av att upprätthålla kritisk kompetens och skapa nätverk understryks inom den finländska statsförvaltningen även därför att systemen är decentraliserade.

I kommunikationsutskottets utlåtande (27/2013 rd) förutsattes att resursbehovet för cybersäkerhetsfunktionerna följs upp och att om uppgifterna ökar till följd av förändringar i omvärlden bör detta beaktas i resurstilldelningen och finansieringen. På basis av revisionsiakttagelserna är det oklart om utlåtandet har beaktats tillräckligt.

I bestämmelserna och processerna för beredning av statsbudgeten kan man inte identifiera förfaranden som skulle säkerställa att anslagen riktas till de viktigaste objekten med tanke på cyberskyddet som helhet. Ämbetsverk och inrättningar budgeterar anslagen för cyberskydd ospecificerat på omkostnadsmomentet som en del av utgifterna för hela verksamheten. Avgifterna för cyberskyddstjänster påverkar efterfrågan på Cybersäkerhetscentrets cyberskyddstjänster och centrets förutsättningar att tillhandahålla tjänster och upprätthålla en hög kunskapsnivå. Ämbetsverkens och inrättningarnas beroende av varandra bl.a. genom servicecentren samt deras vilja och möjligheter att skaffa avgiftsbelagda cyberskyddstjänster från Cybersäkerhetscentret med anslag på omkostnadsmomentet återspeglas i slutändan på centrets förutsättningar.

Åtgärder enligt strategin för cybersäkerheten i Finland vidtas endast inom den ram som anslaget tillåter. Väsentliga åtgärder med tanke på försörjningsberedskapen och indirekt även för cyberskyddet i statsförvaltningens har dock kunnat säkerställas med finansiering från Försörjningsberedskapscentralen.

Cyberskyddet bör beaktas vid IKT-omorganisationer

IKT-omorganisationer inom statsförvaltningen har påverkats organiseringen av cyberskyddet. Administrativa och praktiska cyberskyddsåtgärder har centraliserats till Valtori men startskedet för Valtori har blivit längre än planerat och under denna tid har man haft svårigheter att hålla organiseringen av cyberskyddet på den ursprungliga nivån. Det har visat sig svårt att utveckla det cyberskydd som centraliserats till Valtori. På praktisk nivå har det funnits brister i bedömningen av skyddsförfarandenas tillräcklighet och i införandet av nya arrangemang.

Skäl att förbättra framtagningen av den operativa lägesbilden

Myndigheternas lägesbilder över cybersäkerheten stöder organiseringen av cyberskyddet. Cybersäkerhetscentret upprätthåller den nationella lägesbilden över cybersäkerheten. Med hjälp av centrets lägesbild kan myndigheterna åtgärda sårbarheter i program samt skapa beredskap för och reagera på pågående cyberangrepp.

Ju bättre täckning lägesbilden har, desto bättre tjänar den organiseringen av cyberskyddet. De som blir föremål för cyberangrepp har ingen skyldighet att anmäla angrepp till Cybersäkerhetscentret. Anmälningsskyldighet för organisationer i statsförvaltningen liksom mer heltäckande, centraliserade förfaranden för att upptäcka cyberangrepp skulle förbättra lägesbildens kvalitet.

Revisionsverkets rekommendationer

Revisionsverket rekommenderar att

1. finansministeriet fastställer och genomför en operativ hanterings- och ledningsmodell för IKT-tjänster inom statsförvaltningen avseende omfattande cyberstörningar
2. finansministeriet utreder hur cyberskydd av tjänsterna bör beaktas i finansieringen av dem under hela livscykeln
3. Valtori förbättrar genomförandet, utvärderingen och utvecklingen av förfarandena för cyberskydd och för att upptäcka cyberangrepp
4. finansministeriet förbättrar framtagningen av den operativa lägesbilden över cyberskyddet genom att instruera myndigheterna att anmäla cyberangrepp till Cybersäkerhetscentret.